Integrated photonic devices for measurement-device-independent quantum key distribution

Henry Semenenko[1,2], Philip Sibson[2], Mark G. Thompson[2] and Chris Erven[2]

[1] *Quantum Engineering Centre for Doctoral Training, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Tyndall Avenue, Bristol, BS8 1FD, UK*

[2] *Quantum Engineering Technology Labs, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Tyndall Avenue, Bristol, BS8 1FD, UK*

henry.semenenko@bristol.ac.uk

Abstract: We experimentally demonstrate integrated photonic devices for measurement-device-independent quantum key distribution with state of the art error and clock rates which will lead to more cost effective, practical, and secure communication.

OCIS codes: 130.3120 Integrated optics; 270.5568 Quantum cryptography; 270.5565 Quantum communications.

1. Introduction

Quantum key distribution (QKD) has been demonstrated as a promising method to share secret keys for symmetric encryption algorithms in a post-quantum world using single photons sent over a quantum channel. Integrated photonic devices provide a scalable, phase-stable, robust platform for quantum technologies, and a route to commercial systems [1]. In particular, they will provide an accessible way of making QKD systems more widely available.

Recently, QKD has been under scrutiny from the emerging quantum hacking community who have demonstrated that real-world physical implementations do not always match the assumptions of the theoretical models [2]. Measurement-device-independent QKD (MDI-QKD) is a recent protocol that tackles some of the more prevalent attacks on systems by removing detector side-channels [3]. It does so by introducing a third party (Charlie) who acts as a relay to mediate detection events by announcing quantum correlations between states sent by Alice and Bob. The detection events alone do not contain information about the secret key, so an eavesdropper cannot gain information by targeting the detectors. The protocol also lends itself to a star-shaped topology with Charlie as a shared relay, where the detectors and other expensive, complex equipment can be shared between users. By design, this provides a practical, accessible metropolitan network without reducing security by introducing trusted nodes.

We have previously demonstrated chip-based QKD using indium phosphide (InP) transmitters with state of the art key rates and errors comparable to commercial devices [4]. Here we present work towards the use of InP transmitter devices for MDI-QKD further reducing a major barrier to metropolitan quantum secured communication.

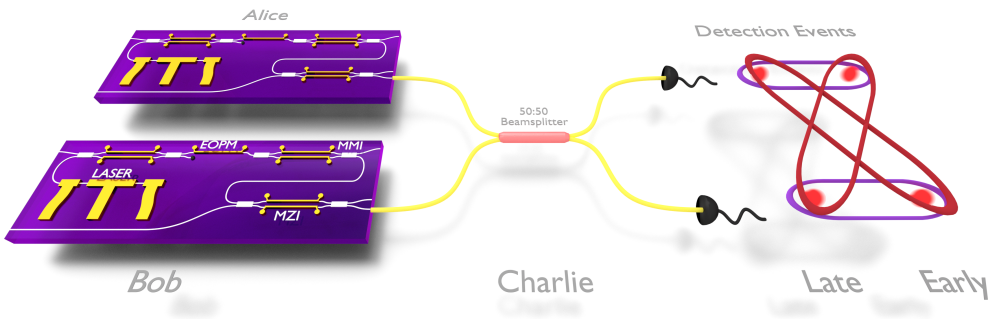

Fig. 1. Two 6×2 mm^2 InP chips create weak coherent QKD states which interfere on a fibre beam splitter. Detector coincidences (shown on the right) indicate successful Bell-state measurements.

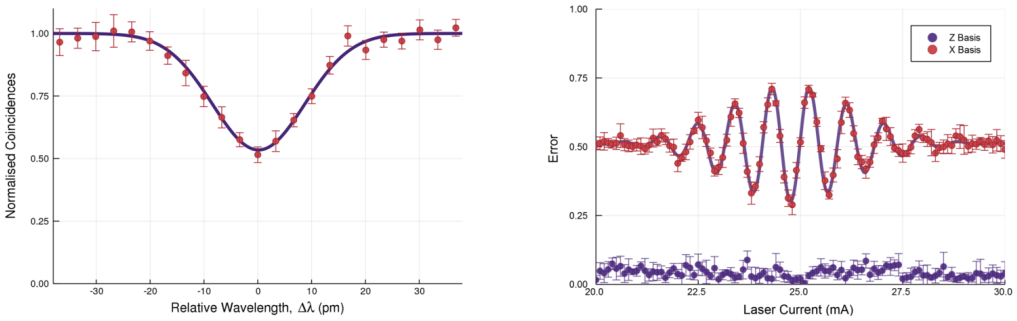

Fig. 2. (Left) Hong-Ou-Mandel interference between two InP transmitters with a visibility of 46.5%. (Right) Bell-state measurements wavelength sweep demonstrating 27% phase error in the X basis, close to the 25% minimum, and low bit errors of $\sim$ 3% in the Z basis.

2. Methods and results

InP is a promising platform for future quantum communication protocols due to the monolithic inclusion of lasers and high-speed (up to 40 GHz) electro-optic modulators [5]. Using integrated Mach-Zehnder interferometers (MZIs), we can temporally modulate 100 ps weak coherent states and encode phase, thus generating high-fidelity time-bin encoded BB84 states at GHz clock rates. The inherent phase-stability and robustness make it a good candidate to facilitate wide-scale quantum key distribution.

MDI-QKD depends on Hong-Ou-Mandel interference [6] at Charlie to produce coincidence events that indicate Bell-state measurements. These correlations can be used by Alice and Bob to generate a secret key. Therefore, we require Alice and Bob to produce states that are indistinguishable to maximise interference. For this, we need to take into account the temporal, intensity, polarisation and wavelength degrees of freedom.

Temporal overlap is controlled using a synchronised clock between the pulse pattern generators and tunable 1 ps resolution delays to ensure that the pulses arrived at the beam splitter simultaneously. Variable optical attenuators were used to match the intensities between the two transmitters and polarisation control and polarising beam splitters were used to overlap the polarisation modes. The experimental setup is shown in figure 1.

Through current injection of the integrated lasers, we can tune the wavelength in steps of 80 fm through a range of $\sim$ 80 pm. This creates the indistinguishable pulses demonstrated in figure 2. We achieve a 46.5$\pm$0.8% visibility compared to the theoretical maximum visibility of 50% when using weak coherent states [7]. We also demonstrate the capability of the on-chip phase encoding that allows error rates of 27% in the X basis. The error is limited to a minimum of 25% due to the 50% visibility limit. The X basis is used to bound knowledge gained by an eavesdropper, whilc the Z basis is used to generate the secret key. The quantum bit errors (Z basis) are around 3% and will be sufficient to generate a positive key rate at competitive speeds.

Demonstrating this interference and error rate is a crucial step towards performing MDI-QKD with integrated devices. It marks a step toward providing ubiquitous quantum secured communication through a scalable integrated platform. Together with wavelength division multiplexing to increase rates and silicon integrated detectors, these devices will facilitate universal access to the quantum internet.

References

1. M.G. Thompson *et al.* Integrated waveguide circuits for optical quantum computing. *IET Circuits, Devices & Systems*, 5:94–102(8), 2011.
2. H.-K. Lo *et al.* Secure quantum key distribution. *Nature Photonics*, 8:595 – 604, 2014.
3. H.-K. Lo *et al.* Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, 2012.
4. P. Sibson *et al.* Chip-based quantum key distribution. *Nature Communications*, 8:13984, 2017.
5. M. Smith *et al.* An introduction to InP-based generic integration technology. *Semiconductor Science and Technology*, 29(8):083001, 2014.
6. C. K. Hong *et al.* Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.*, 59:2044–2046, 1987.
7. J. G. Rarity *et al.* Non-classical interference between independent sources. *Journal of Optics B: Quantum and Semiclassical Optics*, 7(7):S171, 2005.